Introduction of JAXA's IV&V manual

2011 Annual Workshop on Validation and Verification

@West Virginia University Erickson Alumni Center

Hiroki Umeda, Tsutomu Matsumoto

{ umeda.hiroki, matsumoto.tsutomu } @jaxa.jp

JAXA's Engineering Digital Innovation Center (JEDI)

Japan Aerospace Exploration Agency (JAXA)

September 14, 2011

Outline

1. Background
   - -IV&V Research topics in JAXA
2. Introduction of JAXA's IV&V manual
   - -Objectives
   - -Coverage area
   - -Approach
   - -IV&V attributes
3. Case Example
4. Conclusion and Future Work

1. Background

Current IV&V Research topics in JAXA

(1) Developing the Framework to keep high quality of IV&V activity
- IV&V Decision Making Criteria
- **IV&V Manual**
- Measurement of IV&V Effectiveness

To improve Cost Effectiveness

To maximize the accumulated know-how

(2) Developing new IV&V methodology based on project's needs
- Safety Analysis
- Model Based IV&V
- Independent Verification Environment

Discussion Points of this presentation

(1) Concept of JAXA's IV&V manual
- IV&V attributes

(2) Approach to making IV&V manual

2. Why do we need IV&V manual ?

Objectives of IV&V manual

(1) We promote utilization to enhance effectiveness of IV&V.

(2) We generalize IV&V to increase IV&V contractors in Japan

before **IV&V guideline**

We arrange and accomplish IV&V knowledge to inherit it.

now **IV&V manual**

-We focus on utilization of IV&V manual.

- What points should we assess ?
  It introduce IV&V attributes structured.

2-1 Objectives of IV&V

1 Raising dependability of the software

Accuracy
- Assessing accuracy of artifacts objectively.

Completeness
- Assessing enough robustness for failure and fault , and completeness of design .

2 Reduce possibility that satellite system faces critical situation

Safety
- Assessing identified hazard for enough.
- Assessing the software that don't cause hazard .
- Assessing that software satisfy Safety Policy.

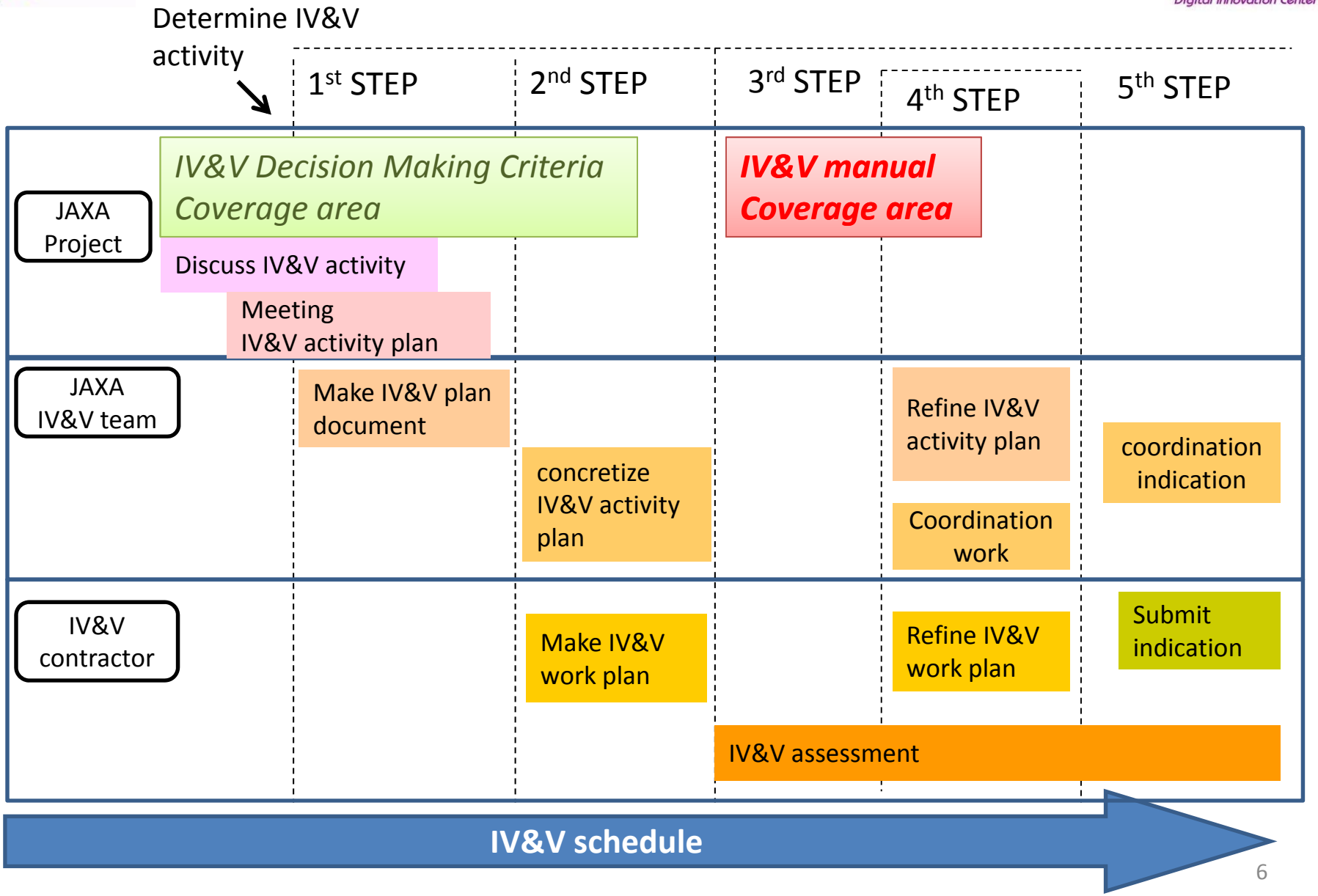
3 Finding the issue of requirement and development in early design phase.

Integrity
- Assessing that the artifact includes in comprehensive and consistently requirement.

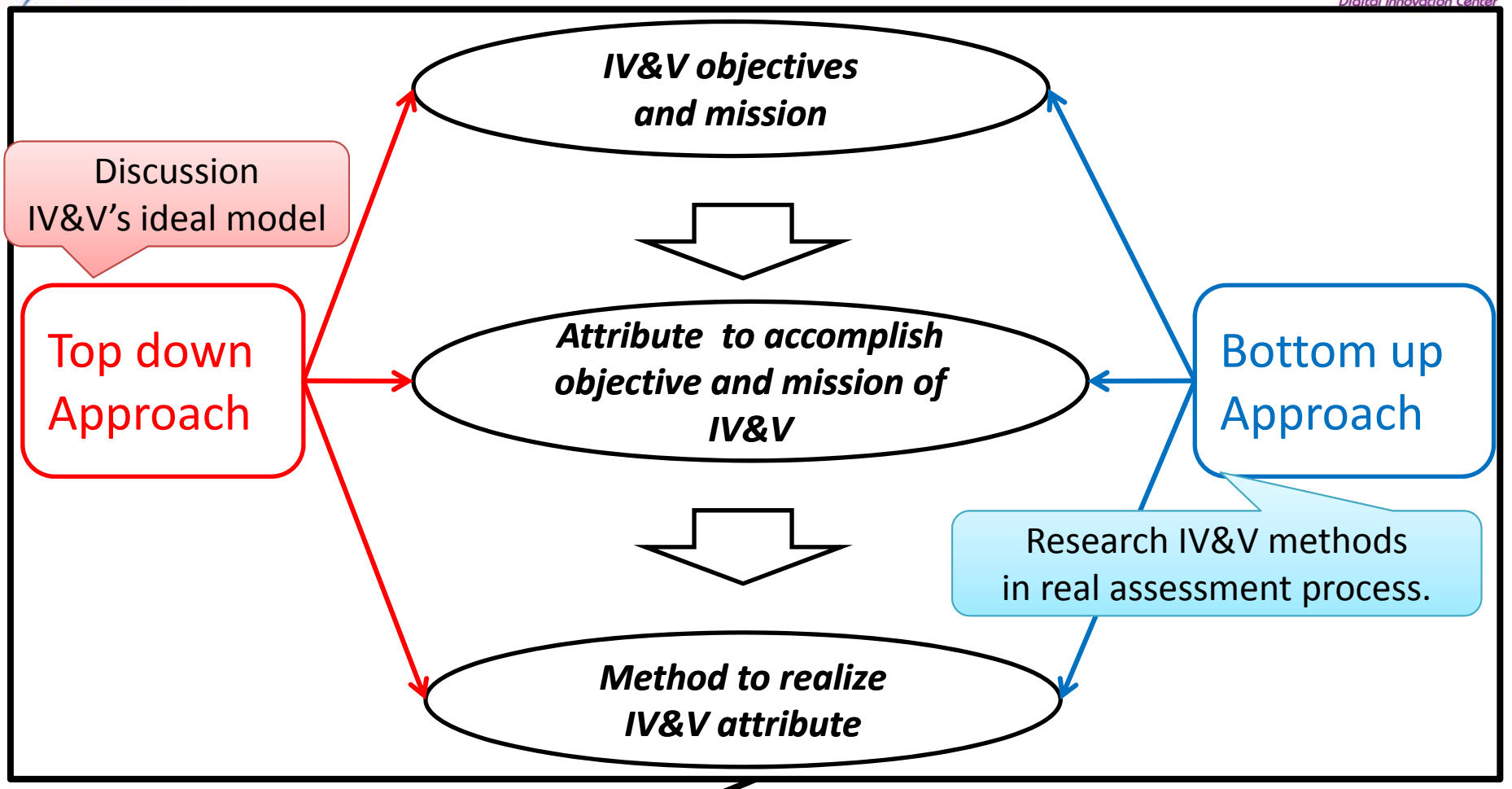
Validation
- Assessing that the software correspond to requirement for system.

Accomplish the mission by increasing dependability of the software

2-2 IV&V manual Coverage area



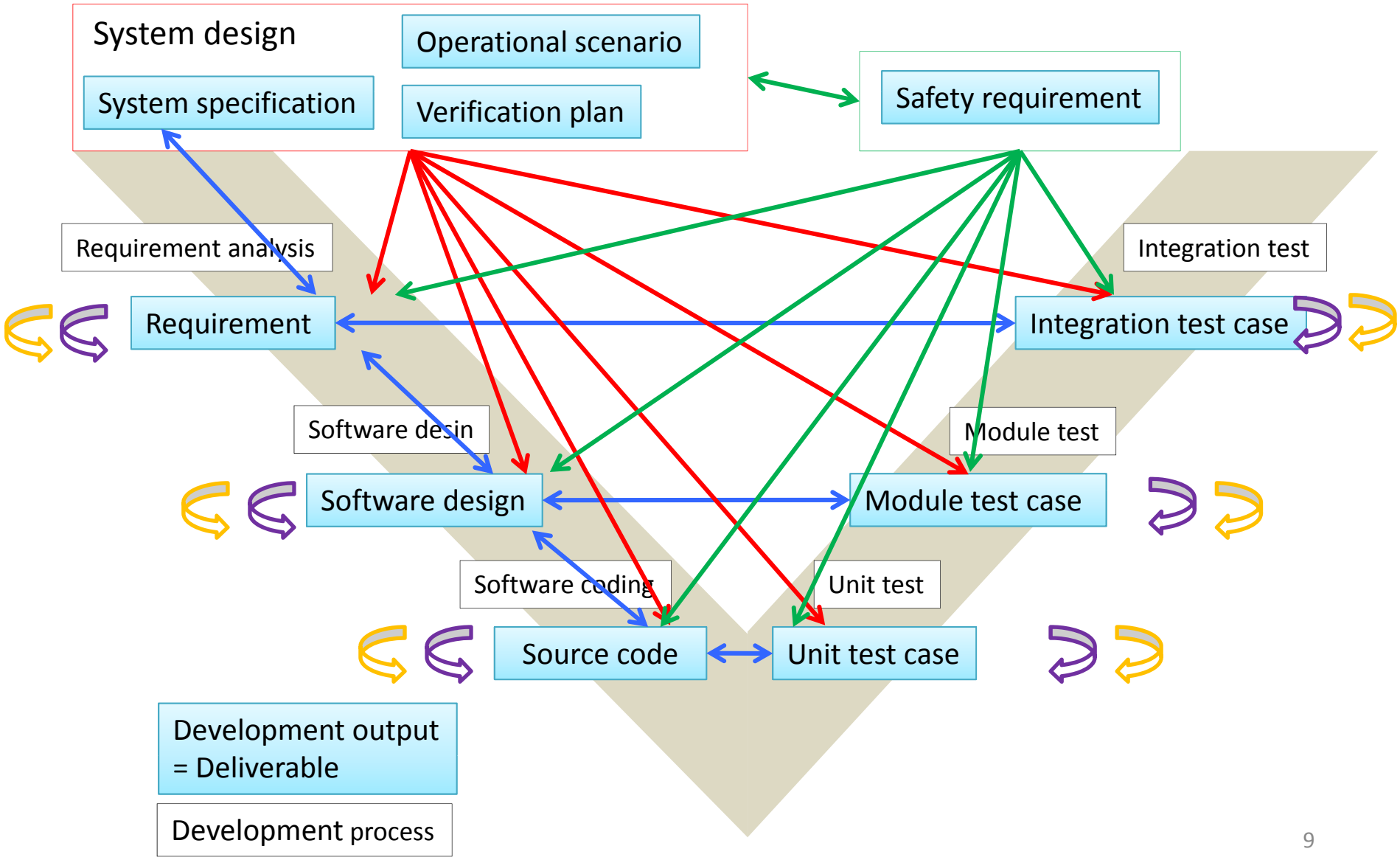
2-3 How to produce IV&V manual



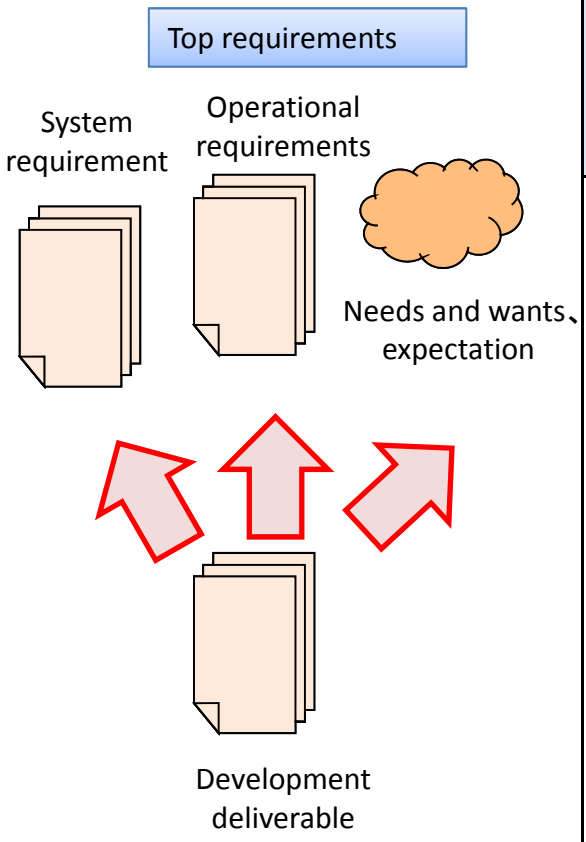
3. IV&V attributes (5 view points)

Validity	Does the artifact satisfy the top level requirement ? * Top level requirement means system/sub system design.
Integrity	Does the artifact include in all requirement for software through development process ?
Accuracy	Is the artifact described correctly ?
Completeness	Does the artifact include all requisite specification (including off nominal and failure tolerability) without omission ?
Safety	Does the artifact satisfy safety requirement and identify all hazard?

3. Relationship between IV&V attributes and artifacts

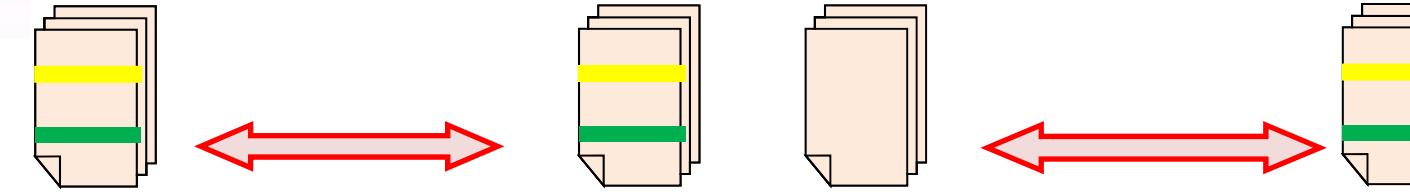


3-1 Validity



attribute	content	
	sub attribute	**explanation**
Validation	Adequacy for system and software requirements	- The performance and function defined in each deliverables satisfy software requirements that system require. - The performance and function defined in each deliverables accord requirements and constraint that system should accomplish.
	Adequacy for operational requirements	-The performance and function defined in each deliverables satisfy realization of system operation. - Deliverables satisfy operational constraints.
	adequacy implicit requirements in deliverable	Deliverables reflect all requirements to develop adequate system where it's not defined about top level requirements and constraints.
	validation of verification	- Based on verification policy, verification for software should be exhaustive and consistency through a whole verification activity - verification activity for software accord real-operation.

3-2 Integrity

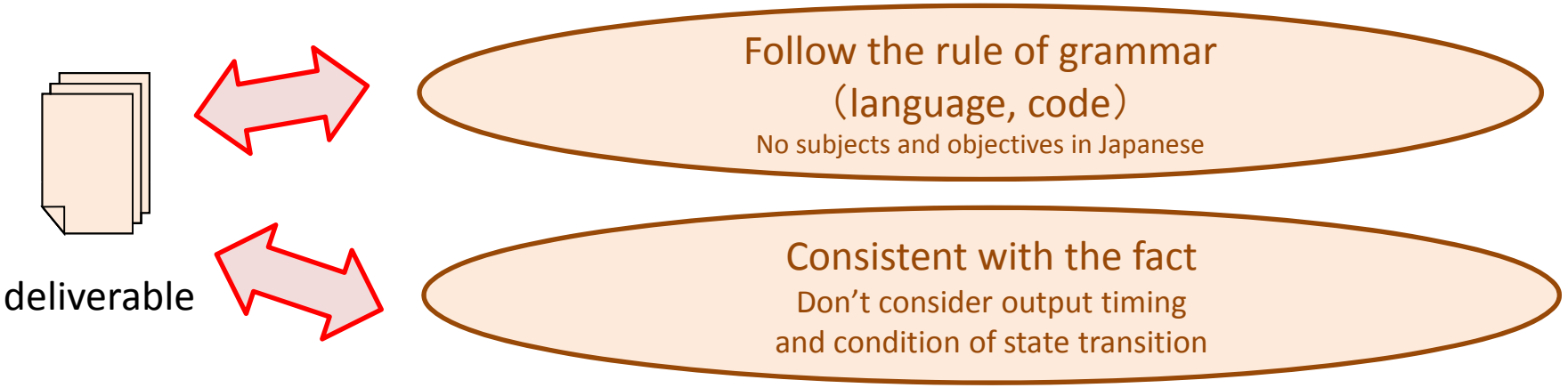


All software requirements reflect development deliverable without omission through development process.

attribute	contents	
	sub-attribute	explanation
Integrity	traceability upper level and lower level	lower level specification in development deliverable include in all items of all upper specifications. all upper level specification correspond to lower level specification without omission. In addition lower level specification correspond to upper level specification.
	equality of upper and lower level	where each specification has traceability upper and lower level specification, total specification in each lower specification equal upper specification.
	traceability of deliverable and interface specification	deliverable reflects all interface specification without omission. In addition, all specifications about all interfaces in deliverable correspond to interface specification.
	equality of deliverable and interface specification	where specification in deliverable and interface have traceability, each contents of both specification are equality. behavior of both specification isn't inconsistency.
	traceability of requirement and testing	All requirements in deliverable correspond to test case in deliverable about verification in deliverable.

3-3 Accuracy

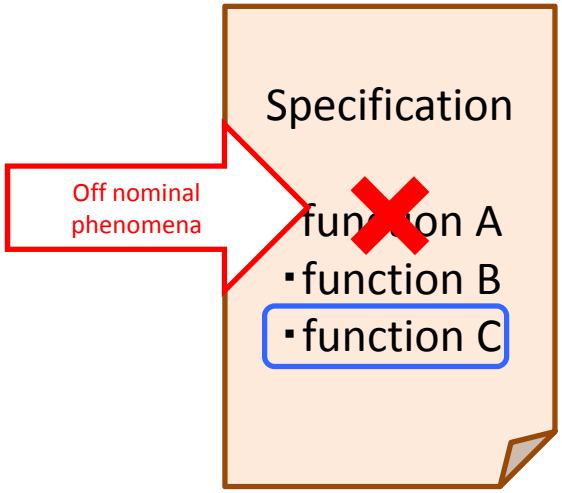
Is one of deliverable（specification, source code）correct ?



1st Attribute	Contents	
	2nd attribute	explanation
Accuracy	consistency of interpretation	One of description (including value and figure) in the deliverable can interpret underspecified.
	consistency of each requirements	inconsistent description that relationship a requirement and negative requirement are true at same situation don’t exist in deliverable.
	coverage of condition	Condition about requirements in deliverable is exhaustively considered within the deliverable.

3-4 Completeness

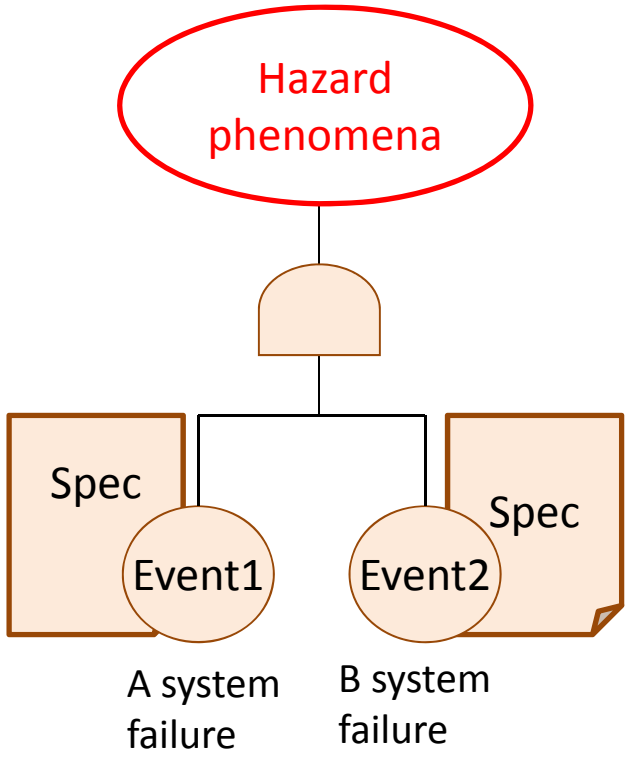
Is off nominal situation considered in design process ?



Does a function (or processing) have adequate behavior within the function ?

attribute	contents	
	sub -attribute	explanation
Completeness	completeness of sate	Inconsistent sate doesn't exist at the same time, it's no possible that the state changes multiple states. All sate changes are defined under expected condition.
	completeness of processing	Processing start at intended timing. After processing properly complete, it terminate in intended timing. Software processing (exception handling, detection, warning etc) properly execute for stop and start of unintended processing.
	completeness of output and input	Date input and output execute at intended timing. Software processing (exception handling, detection, warning etc) properly execute for data input at unintended timing, data input of unexpected value.

3-5 Safety



Doesn't satellite system face critical condition ?

In JAXA IV&V, Safety is not only covered with human life but also lost of satellite and mission regard as hazard.

attribute	contents	
	sub-attribute	explanation
Safety	sufficiency hazard analysis	Identify all the scenario that satellite system comes critical state.
	avoidance hazard	If satellite system come off nominal state, it's specification that avoid critical sate and hazard.
	validation of dealing with off nominal	The system detect all failure and error, in addition system detect off nominal events and states, the specification is adequate processing (informing).

3-6 Case Example

Process	Requirement Analysis	Attribute	Integrity	Sub Attribute	Traceability upper level and lower level

Detailed Attribute

- Outline of attribute (What do we assess in this attribute)

Applicable IV&V Methodology

[Assessment Procedure] - How do we assess in this attribute.

[Technical know-how] - way to assess more efficiency and effective.

[Complementary information]
- It's described in detail and points to be noted in assessment

Previous IV&V Findings

- IV&V outcome in the past projects.

refer to accumulated know-how in the past projects

4. Conclusion and Future Work

Conclusion

JAXA's IV&V manual is being created based on 5 IV&V attributes derived by top-down approach (based on ideal IV&V model) and bottom-up approach (based on IV&V experiences)

- Validity
- Integritiy
- Accuracy
- Completeness
- Safety

Future Work

(1)IV&V manual will be applied to real projects as a trial
- to brush-up the manual by reflecting the practical experiences
- to accumulate and maximize the technical know-how in the manual

(2)IV&V manual and IV&V decision making criteria will be coordinated to achieve cost-effectiveness of IV&V activity.

END